ESET Tech Center

Knowledgebase > Legacy > Locate unprotected computers on your network in ESET PROTECT (8.x)

Locate unprotected computers on your network in ESET PROTECT (8.x)

Steef | ESET Nederland - 2021-05-26 - Comments (0) - Legacy

lssue

- Synchronize ESET PROTECT with Active Directory
- Filter the static group of computers for unmanaged computers
- Use Rogue Detection Sensor (RD Sensor) to populate a list of devices that are not in Active Directory

Solution

Synchronize ESET PROTECT with Active Directory

This ensures that any recently added computers show up in ESET PROTECT.

- 1. Open the ESET PROTECT Web Console in your web browser and log in.
- 2. <u>Create a task to synchronize ESET PROTECT with Active Directory</u>.
- 3. Click Tasks → Server Tasks → Static Group Synchronization.
- Select the check box next to the task you have created and click Actions → Run now. ESET PROTECT automatically adds unmanaged computers from your Active Directory to the All group.



Filter the static group of computers for unmanaged computers

This process will only display computers that are joined to the Domain on your network. To

display computers on your network but not joined to the Domain, <u>Rogue Detection Sensor is</u> <u>needed</u>.

- 1. Click **Computers** and select the **All** group.
- 2. Select the Errors (A), Warnings (9) and OK () icons.
- 3. Select the check box next to **Show Subgroups**.
- 4. In the Security Product column, click Security Product to sort by a security product. It may be necessary to click twice to get the small triangle icon next to Security Product to point up. Any unprotected computers on the network are displayed at the top of the list.

(CS)	D PROTECT			2	3										LOGOUT >52 min
::	DASHBOARD	Computers	:	A O 🗸 O	SHOW SUBGROUPS	🗹 🖿 Al (4)			ADD FILTER				4	PRESET	s• 0
뎍	COMPUTERS	Groups	ب	COMPUTER N/	ME	TAGS	STATUS	MUTED	MODULES	LAST CONNECTED	ALERTS	DETECTIONS		SECURITY PR	GRC 🔘
			0	🕑 win-10-ka	erde-v1 10.1.202.88		0		Unknown	2021 May 12 12:28:26	1	0			Lost & found
X B E ⊕ ⊕ ⇒ ::		Carl A fand (0) Carl A fand (0) Carl A fand (0) Viewees campos Viewees campos Viewees (settop) Viewees (settop) Viewees (settop) Viewees (settop) Viewees (settop) Campose with outdated endostes Campose with outdated endostes Viewees (settop) Viewees (settop)			0.12028	D	• • •		Urknown Urknown Updated Updated	2021 May 12 12:00.00 2021 May 12 12:00.00 2021 May 12 12:00.00 2021 May 12 12:00.00		0	EST Engount Security EST Engourt Security	8.0.2028.0	Lost & found Lost & found Lost & found Lost & found
		This is where you can set the lot of your applied tags and quickly filter thans.	<	ADD NEW 🗢	TIONS 🔻 M	UTE V							_		100

Use Rogue Detection Sensor to populate a list of devices that are not in Active Directory

<u>Rogue Detection Sensor</u> is automatically installed as part of ESET PROTECT package installation and begins working as soon as ESET PROTECT Server is activated. If there are multiple network segments, RD Sensor must be installed separately on each network segment to produce a comprehensive list of all devices on the whole network

Follow the instructions below to find new computers on your network using RD Sensor in ESET PROTECT Web Console:

 Click **Reports**. In the **Computers** section, navigate to **Rogue computers** report. Click the Gear icon ⁽²⁾ and click **Generate Now**.

csei	PROTECT					G ▼ Computer Name	QUICK LINKS 🛩 💿 HELP 🗢	ADMINISTRATOR ☐ LOGOUT
	DASHBCARD	Categories & Templates Scheduled Reports						
돠	COMPUTERS	Templates ACCESS GROUP Select	Taga					0
▲	DETECTIONS	Antivirus detections	Breakdown of installed ESET Applications	Check Detection Engine version	Computer last connection	Computer statuses overview	Computers first time connected in last 7 days	Computers grouped by hardware detection reliability
<u>ي</u>	Reports	Audit and License Management	Doughnut chart which displays the share of the installed ESET Applications		by the last connection time	computer status	List of computers from where ESET Management Agent has first time connected to E	status Computers grouped by their hardware reliability status.
Ð	Tasks	Automation						Hardware reliability sta
	Installers	Computers	m		m @			
۲	Policies	Dynamic Threat Defense	Construction of the	Consultant and the designs	Construction of the section of the s	Constant and the second second		
¢	Notifications	Email servers	cloning	questions	Operating system or managed	hardware detection	ratio	Appliances statuses overview
8-	Status Overview	Enterprise Inspector	List of computers that are set as masters for cloning. Cloning and	List of computers that have unresolved cloning questions. This	products reported problems, with their detail descri	List of computers, which are not providing enough information fo	Ratio between updated and not updated detection engine	Count of EVSAs grouped by their status
	More >	Firewall detections	re-imaging co	might indicate th		reliable hardiw	reported by security prod	
		Full Disk Encryption		m	m (h)			
		Hardware inventory	ESET Victor Patient Security	Installed applications	Installed applications in last 7	Installed applications on mobil	Installed ESET applications	last undate
		Network	Appliances with problems	Overview of installed applications	days	devices	Overview of installed applications	Computers grouped by the last
		Quarantine	Operating system of unaged products reported problems, with	on computers. By default, only ESET applicati	Overview of applications installed on computers within last 7 days.	Overview of installed applications on mobile devices. By default, on	y applications are repo	detection engine update
		Server performance	their detail descru.		By default,	ESET appL.		
				•	O O	O O	o O o	
			List of computers with identity	Mobile device detection engine	Mobile device last connection	Mobile device last update	Mobile devices statuses	Mobile devices with problems
			List of computers with identity	Ratio between updated and real	Overview of mobile devices grouped by the last connection	Mobile devices grouped by the last detection engine update	Rogue computers Jerns reported	Operating system or managed products reported problems, with
			recovered in last 7 days. Computers for which th	updated detection engine reported by security prod	time		Generate Now or managed	their detail descri
							Download P Schedule	
			۵	(🖉 🖉 Edit. 💿	۵
			Not connecting computers	Operating systems	Outdated applications	Rogue computers	Audit Log ratio	Static groups with unresolved
			Overview of computers not connecting for more than 14 days	Overview of operating systems on computers	Overview of outdated applications on computers	s Computers detected by Rogue Detection Sensor, that do not have	e B Delete 35	Report displays static groups, with
						an entry in c5c1	Export	number or detections that are in not resolve
			Θ	Θ	Θ		⊎ (G	
	COLLAPSE		Top agentiess virtual machines	top computer problems	top mobile devices problems	Unresolved cloning questions	virtual machines with no agent -	web Control Logs

2. The report shows a list of unmanaged computers, as well as all devices connected to the network (including routers, printers or cameras etc.) The Admin may need to verify the IP addresses in the list since it may include non-Windows devices that do not need to have an ESET product installed. Click the computer you want to add and click Add to add computers to ESET PROTECT individually. Alternatively, you can click anywhere in the list and then click Add all displayed items.

< BACK REFRESH	GENERATE AND DOWNLOAD	SCHEDULE				
Report: Rogue compute	ers					
Server Name protect.local						
Generated at 2021 May 12 14:36:55 (UTC+02:0	0)					
Number of records 97						
Filters						
MAC address	Pv4 address	IPv6 address	Alternative host names	Host name	Network adapter vendor	Detected OS
00-50-56-98-A9-42 ; Unknown computer						_
+ Add						
+ Add all displayed iten	15					
the size of the second						
	100000000000000000000000000000000000000	and a second second second	the second second	and the second second	Concerning and	

3. Review the list of computers to be added (to remove them click the trash bin icon in next to a computer), then click **/All** to select a Parent Group to which the computers will be added (by default, this is the **All** group) and click **Add**.

< BACK Reports > Show Report > Add Computers
Add Computers
Create or import a list of computers. In the next step you can deploy an agent to connect and manage them in ESET PROTECT.
List of devices
NAME DESCRIPTION Remove All WMM III IIII + ADD DEVICE IMPORT CSV COPY & PASTE
Tags
Select tags
Settings
Parent Group /All
Use FQDN resolution
Conflict Resolution
Ask when detected
ADD CANCEL

4. Click **OK** to add the computers. To <u>send the ESET Management Agent to these</u> <u>unmanaged computers</u> click **Deploy Agent**.

